PROCEDURA DI GESTIONE DELLA *PRIVACY*

ATTESTAZIONE

Il personale della SGR ha la responsabilità di acquisire un'adeguata conoscenza della presente procedura (e degli eventuali successivi aggiornamenti) e di seguire, senza eccezioni, la procedura in essa descritta. Si prega, pertanto, di leggere accuratamente la procedura e di attestarne il ricevimento e l'impegno a seguire le regole in esso contenute firmando questa attestazione e restituendola al Responsabile della Funzione di *Compliance.*

* * *

Il sottoscritto dichiara di aver ricevuto una copia della "Procedura di gestione della *Privacy*". Il sottoscritto dichiara inoltre che rispetterà la procedura in epigrafe nei suoi eventuali aggiornamenti, recependo altresì le indicazioni contenute nei *memorandum* interni aziendali.

Nome e cognome: _____

Data: _____

Firma: _____

INDICE

1. PREMESSE E OBIETTIVO DELLA PROCEDURA

La presente Procedura persegue l'obiettivo di descrivere gli adempimenti in carico ad Alisei SGR S.p.A. (di seguito anche la "Società" o la "SGR") al fine di definire le misure di sicurezza idonee a garantire la corretta gestione dei dati personali trattati, all'esito di un'attenta analisi dei rischi.
Al fine di assicurare una migliore tutela della *Privacy* e del trattamento dei dati personali nella UE, nonché per armonizzare e aggiornare le differenti normative nazionali allo scopo di favorire la creazione di un unico mercato digitale europeo, in data 24 maggio 2016 è entrato in vigore il Regolamento europeo 2016/679 in materia di protezione dei dati personali (di seguito anche "Regolamento" o "GDPR"), effettivamente applicabile dal 25 maggio 2018.
La presente Procedura regola il trattamento dei dati personali, da chiunque effettuato nel territorio dello Stato, con o senza mezzi elettronici, o comunque automatizzati, ai sensi del D.Lgs. 30/06/2003 n. 196 Codice in materia di protezione dei dati personali (di seguito anche "Codice Privacy"), del D.Lgs. 10/08/2018 n. 101 di adeguamento del "Codice *Privacy* e del Regolamento europeo 2016/679 in materia di protezione dei dati personali e successive modifiche e integrazioni.
Le norme prescritte dalle suddette leggi e regolamenti intendono garantire che il trattamento dei dati personali si svolga nel rispetto della dignità umana, dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. La tutela si estende anche ai diritti di chi rappresenta le persone giuridiche, gli Enti e le Associazioni.

2. PRINCIPI FONDAMENTI DA UTILIZZARE NEL TRATTAMENTO DEI DATI

Le operazioni di trattamento dei dati svolte dalla SGR includono la raccolta, gestione, archiviazione e conservazione delle informazioni pervenute.
I dati sono raccolti allo scopo prevalente di sottoscrivere i contratti con la Clientela, relativi ai Servizi di Investimento autorizzati, ovvero il Contratto di Gestione di portafogli, il Contratto di Ricezione e Trasmissione di Ordini, il Contratto di Consulenza in materia di investimenti, il Collocamento senza preventiva autorizzazione o acquisto a fermo, ovvero assunzione di garanzia nei confronti dell'emittente (di seguito anche i "Contratti").
La SGR, dopo aver provveduto a illustrare al Cliente il contenuto della documentazione contrattuale (cosiddetta informativa pre-contrattuale), chiede al Cliente un documento di identità e i relativi dati al fine di censire il Cliente in anagrafica e compilare il Contratto. I dati personali oggetto del trattamento devono essere:

- trattati in modo lecito ovvero nel rispetto delle norme;
- raccolti e registrati per scopi determinati, chiari, espliciti e legittimi;
- esatti ovvero rispondenti all'identità o al profilo dell'interessato e, nel caso, aggiornati;
- pertinenti ovvero vi deve essere una chiara e stretta relazione tra i dati raccolti e le finalità del trattamento perseguite;
- completi, in modo da non dar luogo a errori nell'identificazione e individuazione dell'interessato;
- non eccedenti rispetto alle finalità per le quali sono stati raccolti (è il cosiddetto principio di proporzionalità che vieta la raccolta e il trattamento di dati personali che siano superflui rispetto agli scopi dichiarati del trattamento);

- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati stessi sono stati raccolti.

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati. Alla inibitoria all'utilizzo dei dati possono peraltro affiancarsi, qualora ne ricorrano gli estremi, anche ulteriori sanzioni amministrative e penali.
Inoltre nell'ipotesi in cui, per effetto del trattamento di dati personali, sia stato provocato danno ad altri, chiunque abbia cagionato il danno è tenuto a risarcirlo, ai sensi dell'articolo 2050 del codice civile, mentre a carico della Società risulterà anche la responsabilità di cui all'art. 2049 codice civile prevista per padroni e committenti.
I dati sono trattati prevalentemente per finalità contrattuali, nell'ambito dell'attività della Società. Sono anche trattati per finalità connesse e funzionali a quelle contrattuali o per finalità di marketing diretto.
I dati personali relativi alla Clientela sono riferiti alle persone fisiche ed ai rappresentanti o referenti delle persone giuridiche, che afferiscono ai Contratti in qualità di Intestatario, Cointestatario e Delegato a operare sul rapporto, nonché in qualità di Titolare effettivo o Beneficiario dell'operazione.
Per quanto riguarda le persone fisiche, i dati in questione attengono a tutti gli elementi di seguito indicati:

- complete generalità: nome, cognome, luogo e data di nascita, cittadinanza, residenza anagrafica;
- gli estremi del documento di identificazione valido: tipo, numero, luogo, data rilascio, autorità di rilascio, scadenza;
- codice fiscale: deve essere rilevato dal tesserino rilasciato dal MEF o dalla Tessera Sanitaria - Carta Regionale dei Servizi .

Per quanto riguarda le persone giuridiche, va acquisita la seguente documentazione:

- la denominazione o ragione sociale, la sede e l'indirizzo;
- numero di Partita IVA;
- Settore Attività Economica e Ramo Attività Economica (SAE/RAE);
- atto costitutivo;
- statuto;
- visura camerale con l'indicazione dell'assetto proprietario;
- delibera di conferimento dei poteri di rappresentanza;
- copia del documento di identità e codice fiscale di colui che ha i poteri di rappresentanza o è stato delegato a operare;
- oltre all'acquisizione dei dati identificativi, andranno acquisite informazioni circa la sussistenza del potere di rappresentanza.
-

3. PRINCIPALI FIGURE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI

La realizzazione di un idoneo sistema di protezione e salvaguardia dei dati personali richiede, prima di qualsiasi misura, che siano chiaramente definite e individuate le figure interessate al trattamento, i rispettivi ruoli e i relativi diritti e doveri.

Il Codice *Privacy* e il GDPR identificano le seguenti figure:

- Titolare del Trattamento;
- Responsabile del Trattamento;
- Responsabile della protezione dei dati (*Data Protection Officer*)
- Soggetti Incaricati al Trattamento.

3.1 Titolare del trattamento

Titolare del Trattamento dei dati è Alisei SGR S.p.A. nella persona dell'Amministratore delegato dott. Giovanni Penco, che provvede a nominare i suoi Incaricati.

3.2 Responsabile del trattamento

Nel caso in cui, nell'ambito delle attività affidate dalla SGR a Società esterne, queste vengano a trattare dati personali per conto del Titolare, occorrerà nominare tali entità (persone fisiche o giuridiche) Responsabili del Trattamento, tramite formalizzazione di apposito contratto (o altro atto giuridico) di nomina, ai sensi dell'art. 28 GDPR. In tali casi il contratto di collaborazione deve altresì prevedere che la società cui viene affidato l'incarico si impegni ad adempiere alla normativa sulla Privacy tempo per tempo vigente e al GDPR.

3.3 Responsabile della protezione dei dati (Data Protection Officer)

La Società ha designato quale Responsabile della protezione dei dati o *Data Protection Officer* ("DPO"), ai sensi degli artt. 37 e seguenti del GDPR, il Sig. Francesco Cattivelli, che per esperienza, capacità e affidabilità fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Il DPO effettua il proprio compito autonomamente, non ricevendo istruzioni dal Titolare o dal Responsabile del Trattamento. Egli riferisce direttamente al vertice gerarchico del Titolare o del Responsabile.
I compiti del DPO sono quelli indicati nell'art. 39 GDPR ed eventualmente altri che gli vengano affidati e che non diano adito a conflitto di interessi.
Gli interessati hanno la facoltà di rivolgersi direttamente al DPO per ogni questione che riguardi il trattamento dei loro dati personali.
Il DPO è soggetto esterno alla Società e per il compito affidatogli ha diritto ad un compenso contrattualmente stabilito.

3.4 Soggetti Incaricati al Trattamento

Gli incaricati del trattamento sono i soggetti designati dal Titolare a compiere le materiali operazioni di trattamento dei dati personali, ovvero coloro che per conto del Titolare raccolgono dati, li elaborano attraverso i sistemi applicativi o manualmente, li archiviano, li comunicano e li diffondono (ad es. i dipendenti del Titolare).
Gli incaricati possono essere solo persone fisiche e sono designati dal Titolare del Trattamento.
Gli incaricati possono effettuare operazioni di trattamento solo sotto la diretta autorità del Titolare, attenendosi alle istruzioni impartite.

L'Incaricato è tenuto a compiere tutto quanto si renda necessario al fine di rispettare le disposizioni di legge e, a tal proposito, è autorizzato a compiere le operazioni di trattamento dei dati, attenendosi alle istruzioni impartite dalla Società stessa, in qualità di titolare del trattamento.
Ai sensi del Codice *Privacy* e del GDPR i dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tale riguardo, è richiesto all'Incaricato particolare attenzione ai seguenti punti aventi specifica attinenza con la sicurezza dei dati trattati:

- classificazione dei dati personali, al fine di distinguere quelli sensibili (qualora dovesse essere oggetto di trattamento anche detta tipologia di dati), osservando le maggiori cautele di trattamento che questo tipo di dati richiede;
- consultazione dei documenti contenenti dati personali necessari per lo svolgimento dell'attività lavorativa prestando particolare attenzione alla custodia e all'archiviazione degli stessi;
- elaborazione e custodia delle credenziali di autenticazione necessarie per accedere agli strumenti elettronici e ai dati in essi contenuti;
- custodia e accessibilità degli strumenti elettronici mentre è in corso una sessione di lavoro;
- uso degli strumenti e dei programmi in conformità alle policy aziendali al fine di proteggere i sistemi informativi e i dati ivi contenuti;
- utilizzo, custodia e archiviazione dei supporti rimuovibili contenenti dati personali in conformità alle *policy* aziendali.

Al fine della corretta gestione dei dati personali oggetto di trattamento, l'Incaricato dovrà osservare le procedure aziendali per il trattamento dei dati personali con e senza strumenti elettronici e ogni altra indicazione che potrà essere fornita dal Titolare del trattamento.

In particolare, l'Incaricato è invitato ad attenersi alle seguenti indicazioni:

i) Effettuare le operazioni di trattamento e utilizzare le banche dati conformemente all'ambito del trattamento della propria Area, attenendosi alle seguenti istruzioni operative:

- effettuare le operazioni di trattamento solo dei dati personali necessari per lo svolgimento della propria attività lavorativa, nel rispetto del principio di necessità e delle misure di sicurezza predisposte dal Titolare del trattamento a tutela della riservatezza degli interessati;
- non lasciare incustodito il proprio posto di lavoro prima di aver provveduto alla messa in sicurezza dei dati; in caso di allontanamento, anche temporaneo, dal luogo ove si svolge il trattamento dei dati personali, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi non incaricati di accedere ai dati personali per i quali

era in corso il trattamento;
- limitare l'accesso ai dati necessari all'espletamento delle proprie mansioni;
- comunicare e/o diffondere solo i dati personali preventivamente autorizzati dal Titolare;
- custodire e non divulgare le credenziali di autenticazione (User ID e password) di accesso agli strumenti elettronici;
- conservare separatamente eventuali dati sensibili;
- informare prontamente il Titolare e il DPO di ogni questione rilevante ai fini del rispetto della normativa in materia di protezione dei dati personali;
- informare il Titolare e il DPO in merito a qualsiasi richiesta di accesso e di esercizio dei diritti da parte degli interessati entro e non oltre 24 ore dalla ricezione della stessa.

ii) Utilizzare i seguenti strumenti:
- strumenti di comunicazione elettronici attribuiti dal Titolare al singolo incaricato per lo svolgimento delle proprie mansioni lavorative.

Gli obblighi relativi alla riservatezza, alla comunicazione e alla diffusione dovranno essere osservati dagli Incaricati anche in seguito a modifica dell'incarico e/o alla cessazione del rapporto di lavoro.

4. OBBLIGHI DI SICUREZZA

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

È necessario quindi che gli incaricati osservino le norme comportamentali che discendono dalle misure di sicurezza disposte secondo quanto indicato dal Codice *Privacy* e dal GDPR, attenendosi scrupolosamente alle presenti istruzioni e a ogni altra indicazione, anche verbale, che potrà essere fornita dal Responsabile del Trattamento.

Le misure di sicurezza sono specificatamente descritte nel "Disciplinare Tecnico in materia di misure di sicurezza" allegato alla presente Procedura (cfr. Allegato 1).

Di seguito sono indicati alcuni principi e regole fondamentali per il regolare funzionamento, l'affidabilità della gestione e la reputazione della Società, ai quali tutti i componenti degli Organi Amministrativi e di Controllo, i Dipendenti, i Collaboratori e i Consulenti Finanziari della SGR si devono ispirare:
- l'osservanza dell'obbligo di riservatezza sulle informazioni di carattere confidenziale acquisite dagli investitori o di cui dispongano in ragione della propria funzione, per cui tutti i componenti degli Organi Amministrativi e di Controllo, tutti i Dipendenti, i Consulenti Finanziari e i Collaboratori della SGR devono rispettare il segreto professionale per ogni notizia, dato o informazione di carattere confidenziale che sia in loro possesso in ragione della attività svolta;
- l'osservanza dell'obbligo di un corretto trattamento dei dati personali e di un corretto utilizzo degli strumenti e dei servizi informatici, che deve avvenire nel pieno rispetto della procedura aziendale dettata a presidio della raccolta, trascrizione, archiviazione e distruzione dei dati personali, nei limiti dell'autorizzazione rilasciata dai soggetti a

cui detti dati appartengono;
- l'osservanza dell'obbligo di riservatezza sulle informazioni di carattere privilegiato acquisite per ragioni d'ufficio, per cui tutte le informazioni a disposizione di Alisei SGR devono essere trattate nel rispetto della riservatezza e della privacy dei soggetti interessati, eccezion fatta per le comunicazioni richieste per legge.

5. INFORMATIVA

In ogni caso di raccolta di dati personali, deve essere fornita idonea informativa (artt. 13 e 14 GDPR), concisa, chiara, semplice e di facile accesso, ai soggetti interessati in merito a:

- identità del Titolare e del *Data Protection Officer*;
- finalità e base giuridica del trattamento;
- interessi legittimi perseguiti dal Titolare o da terzi;
- destinatari o categorie di destinatari dei dati personali;
- eventuale trasferimento verso paesi extra UE e relativo strumento di liceità;
- periodo di conservazione dei dati e/o criteri per la cancellazione;
- diritti dell'interessato;
- natura del conferimento dei dati e conseguenze in caso di rifiuto;
- eventuale esistenza di processi automatizzati;
- se non acquisiti direttamente, fonte da cui hanno origine i dati.

6. CONSENSO

Il consenso dell'interessato (art. 7 GDPR) è necessario in caso di raccolta e trattamento dei dati personali, che non possieda una diversa base giuridica.
Per essere valido tale consenso deve:

- derivare da atto positivo e inequivocabile
- essere libero, specifico e informato
- essere sempre revocabile (ma i trattamenti precedenti rimangono validi).

È compito del Titolare del trattamento dimostrare che l'interessato abbia prestato il consenso.
Il consenso non è dovuto quando il trattamento:

- è necessario per adempiere a un obbligo previsto dalla legge;
- è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere a specifiche richieste dell'interessato stesso;
- riguarda dati provenienti da pubblici registri, elenchi o atti (fermo restando i limiti di legge sulla conoscibilità e pubblicità dei dati);
- riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo.

Particolare attenzione va posta al trattamento dei dati personali dei dipendenti, sia al momento della loro assunzione, in cui è richiesto il consenso esplicito, sia in caso di differenti modalità di trattamento (es. in caso di videosorveglianza e policy per l'utilizzo di *internet* ed *e-mail*).

7. DIRITTI DELL'INTERESSATO

I diritti connessi ai dati personali che Alisei SGR tratta sono:

- DIRITTO ALLA RETTIFICA. L'interessato può ottenere da parte di Alisei SGR la rettifica dei dati personali che lo riguardano o dallo stesso comunicati. Alisei SGR. compie sforzi ragionevoli per fare in modo che i dati personali in suo possesso siano precisi, completi, aggiornati e pertinenti, sulla base delle informazioni più recenti a disposizione;
- DIRITTO ALLA LIMITAZIONE. L'interessato può ottenere una limitazione al trattamento dei dati personali qualora:
  - Contesti la precisione dei dati personali nel periodo in cui Alisei SGR deve verificarne l'accuratezza;
  - Il trattamento sia illecito e si richieda una limitazione del trattamento o la cancellazione dei dati personali;
  - Non sussista più, da parte di Alisei SGR, la necessità di mantenere i dati personali, ma l'interessato ne abbia bisogno per accertare, esercitare o difendere i propri diritti in sede giudiziaria;
  - L'interessato si opponga al trattamento mentre Alisei SGR verifica se le proprie motivazioni legittime prevalgano su quelle dell'interessato.
- DIRITTO ALL'ACCESSO. L'interessato può chiedere ad Alisei SGR informazioni sui dati personali conservati che lo riguardano, incluse le informazioni su quali categorie di dati personali Alisei SGR possiede o controlla, a quale scopo vengano usati, dove sono stati raccolti (se non direttamente presso l'interessato) e a chi siano stati eventualmente comunicati.
- DIRITTO ALLA PORTABILITÀ. In seguito alla richiesta dell'interessato, Alisei SGR trasferirà i dati personali a un altro Titolare del trattamento, se tecnicamente possibile, a condizione che il trattamento sia basato sul consenso dell'interessato o sia necessario per l'esecuzione di un contratto.
- DIRITTO ALLA CANCELLAZIONE. L'interessato può ottenere da Alisei SGR la cancellazione dei dati personali qualora:
  - I dati personali non siano più necessari in relazione agli scopi per cui sono stati raccolti o altrimenti trattati;
  - L'interessato abbia diritto a opporsi a un ulteriore trattamento dei dati personali ed eserciti questo diritto alla opposizione;
  - I dati personali siano stati trattati in modo illecito.

  A meno che il trattamento sia necessario in virtù di obblighi legali, di legge o al fine di costituire, esercitare o difendere un diritto in sede giudiziaria.
- DIRITTO ALLA OPPOSIZIONE. L'interessato può opporsi in qualsiasi momento al trattamento dei dati personali, alla condizione che il trattamento non sia basato sul proprio consenso (salvo il caso della revoca del consenso), ma sui legittimi interessi di Alisei SGR o di terzi. In tali ipotesi Alisei SGR non tratterrà più i dati personali a meno che sia possibile dimostrare i motivi cogenti e legittimi, un interesse prevalente al trattamento o all'accertamento, oppure l'esercizio o la difesa di un diritto in sede giudiziaria. Qualora l'interessato si opponga al trattamento, dovrà specificare se intende cancellare i dati personali o limitarne il trattamento.
- DIRITTO DI PRESENTARE UN RECLAMO. In caso di supposta violazione della legge o del regolamento vigente in materia di privacy, l'interessato può presentare un reclamo presso le autorità competenti del proprio paese o del luogo ove si sarebbe

consumata la presunta violazione.

I diritti degli Interessati sono peraltro soggetti alle limitazioni previste dagli artt. 2-*undecies* e 2-*duodecies* del Codice *Privacy* introdotti dal D.Lgs. 10 agosto 2018 n. 101, qualora rechino un pregiudizio effettivo e concreto a interessi ritenuti meritevoli di maggior tutela e per ragioni di giustizia.

La Società ha predisposto una procedura di gestione dei diritti degli Interessati previsti dal Regolamento europeo 2016/679 in materia di protezione dei dati personali, con le relative misure tecniche e organizzative implementate per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli Interessati.

La procedura in oggetto, unitamente al Registro dei diritti degli Interessati, ovvero gli Allegati 3 e 4 alla presente Procedura, hanno come scopo quello di assicurare, da parte del Titolare del Trattamento, il rispetto dei termini di risposta in caso di richiesta da parte dell'Interessato, come sancito dal GDPR.

8. RAPPORTI CON IL GARANTE

Il Titolare del Trattamento, ovvero l'Amministratore delegato della Società, e il *Data Protection Officer*, presidiano e svolgono il corretto flusso di informazioni con il medesimo.

9. MISURE DI SICUREZZA

Il Titolare del trattamento - tenuto conto della natura dei dati, dell'ambito di applicazione, del contesto e della finalità del trattamento, dei rischi derivanti per i diritti e le libertà delle persone fisiche - deve adattare e implementare (riesaminando e aggiornando ove necessario) misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio e dimostrare che il trattamento dei dati personali è conforme al Regolamento (principio di *accountability*).

Il Titolare del trattamento mette in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonomizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto, in special modo, dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Le misure di sicurezza sono specificatamente descritte nel "Disciplinare Tecnico in materia di misure minime di sicurezza", ovvero l'Allegato n. 1 alla presente Procedura.

Le misure di sicurezza sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

- con l'ausilio di strumenti elettronici, ovvero mediante elaboratori, sistemi applicativi e qualunque dispositivo elettronico;
- senza l'ausilio di strumenti elettronici, ovvero con strumenti manuali o su supporto cartaceo.

10. REGOLE DI GESTIONE E CONSERVAZIONE DI DATI PERSONALI

La Società utilizza dati personali e sensibili nello svolgimento della normale attività lavorativa. In particolare, i documenti sono trattenuti dalle risorse all'interno degli uffici nei tempi necessari allo svolgimento delle operazioni loro affidate e, successivamente, riposti nell'apposito armadio, la cui chiave è accuratamente conservata.

I dati personali vengono conservati in forma cartacea ed elettronica adottando le misure di sicurezza previste dalla normativa vigente esclusivamente per il tempo necessario al fine di ottemperare agli obblighi di legge all'uopo prescritti.

Va prestata attenzione alla cancellazione delle informazioni che può essere:

- puntuale, qualora il Titolare riceva richiesta specifica da parte del soggetto interessato;
- automatica, alla scadenza prevista di "*default*".

In entrambi i casi la cancellazione definitiva e totale del dato è soggetta ai requisiti di legge applicabili (es. "dati del dipendente" da conservare per dieci anni).

L'intero processo viene gestito dal Titolare in collaborazione con il *Data Protection Officer* (o con eventuali Referenti interni), mantenendo informato il reparto interessato.

11. *DATA BREACH*

Per *Data Breach* si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati dalla Società.

Un *Data Breach*, quindi, non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un *notebook* di un dipendente).

La normativa (GDPR) prevede l'obbligo di comunicare alle Autorità di controllo la violazione dei dati, ma solo se il Titolare ritiene probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati. Tutti i Titolari del trattamento sono soggetti alla norma; la notifica dovrà avvenire entro 72 ore e comunque "*senza ingiustificato ritardo*" (art. 33 GDPR).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati è elevato, allora si dovranno informare anche gli interessati, sempre "*senza ingiustificato ritardo*".

Non è invece richiesta la comunicazione all'interessato nei casi indicati dall'art. 34, cioè quando:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il

sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richiederebbe sforzi sproporzionati; in tal caso si procede a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Come stabilito dalla normativa, vige l'obbligo di tenere un "Registro Violazioni" (cfr. Allegato 2) dove è necessario compilare le seguenti richieste:

- data;
- numero di persone coinvolte;
- natura della violazione;
- descrizione della violazione e dei dati coinvolti;
- conseguenze;
- notifica ai soggetti interessati coinvolti nella violazione;
- notifica al Garante;
- misure di attenuazione.

12. REGISTRO DEI TRATTAMENTI

La Società non è obbligata alla tenuta del Registro delle attività di trattamento dei dati previsto dall'art. 30 GDPR, non essendo nella condizione prevista dal paragrafo 5 della predetta disposizione.

13. VALUTAZIONE D'IMPATTO (DPIA)

La valutazione d'impatto sulla protezione dei dati, prevista dall'art. 35 GDPR, è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali, valutando detti rischi e determinando le misure per affrontarli; è un processo inteso quindi a dimostrare e garantire la conformità.

Diventa necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento possa presentare un rischio elevato. Si elencano di seguito alcune fattispecie a titolo di esempio:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del GDPR o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Contenuti minimi della valutazione:

- descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- valutazione della necessità e delle proporzionalità dei trattamenti in relazione alle finalità;
- valutazione dei rischi per i diritti e le libertà degli interessati;
- misure previste per affrontare i rischi (misure tecniche e organizzative, garanzie).

Per contro, un trattamento può essere comunque considerato dal Titolare tale da non "presentare un rischio elevato". In questi casi il Titolare del trattamento deve giustificare e

documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati, nonché includere/registrare i diversi punti di vista.

Di seguito si riportano alcuni esempi:

- quando il trattamento non è tale da presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo;
- quando le tipologie di trattamento sono state verificate da un'Autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'Autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati.

Alisei SGR, all'atto dell'entrata in vigore del GDPR, ha provveduto a fare effettuare a Xion Informatica S.r.l. una valutazione generale di impatto, in relazione a tutti i trattamenti dei dati personali di cui è Titolare Alisei SGR, comprensiva di *Penetration Test* e del relativo *Report*.

Tale DPIA ha concluso ritenendo "trascurabili" i rischi catalogati all'interno delle categorie di "accesso illegittimo ai dati", di "modifiche indesiderate dei dati" e di "scomparsa dei dati". Il che rende, allo stato e salvo periodica revisione o nuove valutazioni del Titolare, non necessario il ricorso ad ulteriori approfondimenti o alla consultazione di seguito descritta.

14. CONSULTAZIONE PREVENTIVA CON L'AUTORITÀ DI CONTROLLO

Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio, il Titolare, prima di procedere al trattamento, consulta l'Autorità di controllo (art. 36 GDPR).

Se l'Autorità ritiene che il trattamento violi il Regolamento, la stessa ha 8 settimane dal ricevimento della richiesta per rilasciare un parere scritto; inoltre è possibile una proroga di 6 settimane se il trattamento è complesso.

15. SANZIONI

Si rimanda agli appositi articoli del Codice in materia di protezione dei dati personali per le sanzioni previste in relazione a illeciti penali, violazioni amministrative e responsabilità civile per danni. Facendo presente che la relativa disciplina è stata recentemente innovata dal D.Lgs. 10 agosto 2018 n. 101.

ALLEGATO 1

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

(Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni

scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui

sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui al Titolo V del Codice Privacy, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati.

Misure di tutela e garanzia
25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Trattamenti senza l'ausilio di strumenti elettronici
Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotatidi strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

ALLEGATO 2

REGISTRO VIOLAZIONI

Referenti Registro Violazioni (Data Breach)

(artt. 33 e 34 Regolamento UE 2016/679 - GDPR)

Dati identificativi soggetto a cui appartiene il registro	
Nominativo	
Indirizzo/Sede legale	
P.IVA/C.F.	
N. telefono	
Email	
Domicilio digitale (PEC o altro)	

Contitolare del trattamento (se presente)	
Nominativo	
Indirizzo/Sede legale	
P.IVA/C.F.	
N. telefono	
Email	
Domicilio digitale (PEC o altro)	

Rappresentante (se presente)	
Nominativo	
Indirizzo/Sede legale	
P.IVA/C.F.	
N. telefono	
Email	
Domicilio digitale (PEC o altro)	

Responsabile della Protezione dei Dati – DPO	
Nominativo	
Indirizzo	
P.IVA/C.F.	
N. telefono	
Email	
Domicilio digitale (PEC o altro)	

Creato il:	
Aggiornato al:	

Società:	

Anno:	

N.	**Rif.**	**Dettagli della violazione**						**Conseguenze della violazione**	**Misure adottate o che verranno adottate**			
		Data	N. Di persone coinvolte	Natura della violazione	Descrizione della violazione	In che modo si è venuti a sapere della violazione	Descrizione dei dati coinvolti		Tutti gli individui sono stati informati?	Azioni intraprese	Enti di controllo informati	Quando è stata notificata?

ALLEGATO 3
PROCEDURA DI GESTIONE DEI DIRITTI DEI SOGGETTI INTERESSATI

1. OGGETTO

La presente procedura illustra il processo aziendale seguito da Alisei SGR S.p.A. (di seguito anche la "Società" o la "SGR") in merito agli specifici diritti degli Interessati previsti dal Regolamento europeo 2016/679 in materia di protezione dei dati personali (di seguito anche "Regolamento" o "GDPR") e le misure tecniche e organizzative implementate per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli Interessati.

2. SCOPO

La procedura ha lo scopo di assicurare, da parte del Titolare del Trattamento, il rispetto dei termini di risposta in caso di richiesta da parte dell'Interessato, come sanciti dal GDPR.

3. LEGGI APPLICABILI

- "Regolamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali" 2016/679 (GDPR)
- Decreto Legislativo del 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e modifiche (D.Lgs. 10 agosto 2018 n. 101)

Il Regolamento generale sulla protezione dei dati (*General Data Protection Regulation* - GDPR, Regolamento UE 2016/679) stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali dati; inoltre protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. Suddetto Regolamento si applica al trattamento di dati personali, inclusi quelli archiviati.

4. RESPONSABILITÀ E RISORSE

La presente procedura si applica sempre a tutti i dipendenti, collaboratori e società che collaborano con il Titolare del trattamento.

5. DESCRIZIONE DETTAGLIATA

5.1 I diritti degli Interessati secondo il GDPR

Prima di entrare nel merito della trattazione rispetto agli specifici diritti degli Interessati previsti dal GDPR, è

necessario fare delle considerazioni preliminari, valide in generale per tutti i diritti:

- *È opportuno che i Titolari del trattamento adottino le misure tecniche e organizzative necessarie a favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli Interessati che dovranno avere, per impostazione predefinita, la forma scritta (può essere dato oralmente solo su espressa* richiesta dell'*Interessato, ex art. 12, paragrafo 1 e art. 15, paragrafo 3 Regolamento 2016/679).*
- Il termine per la risposta all'Interessato, per tutti i diritti, è di 30 giorni.
- Il Titolare deve comunque dare un riscontro all'Interessato, anche in caso di diniego, motivando la sua intenzione di non accogliere tale richiesta.
- Spetta al Titolare valutare la complessità del riscontro e stabilire l'ammontare dell'eventuale contributo da chiedere all'Interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (art. 12, paragrafo 5 Regolamento 2016/679) ovvero se sono chieste più copie dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3 Regolamento 2016/679); in quest'ultimo caso il Titolare deve tenere conto dei costi amministrativi sostenuti.
- La risposta fornita all'Interessato deve essere intelligibile, concisa, trasparente, facilmente accessibile e deve utilizzare un linguaggio semplice e chiaro.
- Benché sia il solo Titolare a dover dare riscontro in caso di esercizio dei diritti (artt. 15-22 Regolamento 2016/679), il Responsabile è tenuto a collaborare con il Titolare ai fini dell'esercizio dei diritti degli Interessati (art. 28, paragrafo 3, lett. e, Regolamento 2016/679).
- Il Titolare ha il diritto di chiedere informazioni necessarie ad identificare l'Interessato e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (art. 11, par. 2 e art. 12, par. 6 Regolamento 2016/679).
- In caso di supposta violazione della legge vigente, l'Interessato può presentare un reclamo presso le autorità competenti del proprio paese o del luogo ove si sarebbe consumata la presunta violazione.

5.1.1 Diritto di accesso

L'Interessato ha il diritto di ottenere dal Titolare del trattamento conferma riguardo l'esistenza di trattamenti dei dati personali che lo riguardano e, in caso affermativo, accedere ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali (con relative garanzie sul trasferimento);
- laddove possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinarne il periodo;
- l'esistenza del diritto dell'Interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali trattati o limitarne od opporsi al loro trattamento;
- il diritto di proporre reclamo a un'Autorità di controllo;

- qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

5.1.2 Diritto di rettifica

L'Interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo, tenendo conto delle finalità del trattamento.
L'Interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione relativa.

5.1.13 Diritto di cancellazione (Diritto all'oblio)

L'Interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare, senza ingiustificato ritardo, i dati personali se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'Interessato revoca il consenso su cui si basa il trattamento se non sussiste altro fondamento giuridico per il trattamento.
   L'Interessato ha facoltà di revocare il consenso se:
   - l'Interessato ha dato il consenso al trattamento dei suoi dati personali per uno o più scopi specifici;
   - i dati personali rivelano origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale e trattamento dei dati genetici, dati biometrici allo scopo di identificare in modo univoco una persona fisica, dati sulla salute o dati relativi la vita sessuale o l'orientamento sessuale della persona. L'Interessato ha dato esplicito consenso al trattamento di tali dati personali per uno o più scopi specifici, salvo quando la legislazione dell'Unione o dello Stato membro prevede che il divieto di elaborazione delle categorie speciali di dati personali non possa essere revocato dall'Interessato.
c) l'Interessato si oppone al trattamento;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione Europea o dallo Stato membro cui è soggetto il Titolare del trattamento;
f) il genitore può richiedere la cancellazione dei dati personali del figlio minore o sul quale esercita la patria potestà.

Laddove il Titolare del trattamento ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per

informare gli altri Titolari e/o Responsabili del trattamento che stanno trattando i dati personali della richiesta dell'Interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Le precedenti azioni non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dall'Unione o dallo Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
c) per motivi di interesse pubblico nel settore della pubblica sicurezza;
d) per motivi di interesse pubblico, per finalità di ricerche storiche, scientifiche o ai fini statistici, essendo il diritto applicabile suscettibile di compromettere o rendere impossibile il raggiungimento degli obiettivi di tale trattamento;
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

5.1.4 Diritto di limitazione del trattamento

L'Interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'Interessato contesta l'esattezza dei dati personali, e per il periodo quindi necessario al Titolare del trattamento per verificare l'esattezza dei dati personali;
b) il trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il Titolare non ne ha più bisogno ai fini del trattamento, i dati personali sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'Interessato si è opposto al trattamento, in attesa della verifica circa l'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'Interessato.

Se il trattamento è limitato, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'Interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

5.1.5 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il Titolare del trattamento comunica, a ciascuno dei destinatari cui sono stati trasmessi i dati personali, le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma degli artt. 16, 17

paragrafo 1, 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare del trattamento comunica all'Interessato, qualora lo richieda, tali destinatari.

5.1.6 Diritto alla portabilità dei dati

L'Interessato ha il diritto di ricevere, in un formato strutturato di uso comune e leggibile da dispositivo automatico, i dati personali, forniti a un Titolare del trattamento, che lo riguardano e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso dell'Interessato al trattamento dei propri dati personali per una o più finalità specifiche;
b) il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'Interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento a un altro, laddove risulti essere tecnicamente fattibile.

Il diritto alla portabilità dei dati non pregiudica il diritto di cancellazione. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di autorità pubbliche attribuite al Titolare.

Il diritto alla portabilità dei dati non deve ledere i diritti e le libertà altrui.

5.1.7 Diritto di opposizione

L'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano. Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali, salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano, effettuato per finalità compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Qualora l'Interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento.

Il diritto di opposizione è esplicitamente portato all'attenzione dell'Interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione.

5.2 Il flusso interno

Per qualsiasi richiesta di informazione da parte di un Interessato che riguarda i suoi dati personali, la stessa va trattata con immediatezza e comunicata all'indirizzo e-mail alisei@aliseisgr.it e all'indirizzo del *Data Protection Officer* cattivelli@xioninformatica.it.
Il Titolare crea infatti un indirizzo e-mail da comunicare ai soggetti Interessati, così da poter gestire con più ordine e metodo le diverse richieste.
Ogni richiesta viene registrata e numerata in una tabella specifica denominata "Richieste diritti interessati GDPR".
Secondo il GDPR il Titolare del trattamento è tenuto a rispondere alle richieste degli Interessati senza ingiustificato ritardo e al più tardi entro 30 giorni. Per questo motivo ogni persona informata di richieste da parte di un Interessato non deve dare seguito autonomamente alla richiesta, ma deve comunicare immediatamente al Titolare del Trattamento ogni richiesta pervenuta con tutti i dettagli rilevati.
Non è consentito ed è quindi tassativamente vietato per qualsiasi persona che agisca in azienda trasmettere, in qualsiasi modo (posta, e-mail, fax, telefono), dati personali anche se rivolti all'Interessato. Solo il Titolare del Trattamento può trasmettere tale tipo di informazione, verificando l'identità del soggetto Interessato.

5.3 Verifica dell'identità dell'Interessato

A seguito della ricezione di richiesta da parte dell'Interessato, il Titolare deve procedere a verificarne l'identità. Nell'esercizio dei diritti l'Interessato può dare delega o procura scritta a persone fisiche o a persone giuridiche (enti, organismi, associazioni, organismi portatori di interessi diffusi).
Di conseguenza, il riconoscimento da parte dell'Interessato può avvenire mediante due diverse modalità. Qualora la richiesta provenga direttamente dall'Interessato dovrà essere richiesta la fotocopia di un documento di identità in corso di validità dell'Interessato.
Qualora la richiesta provenga da parte di un terzo (incluso un familiare) dovranno essere richiesti:

- fotocopia di documento di identità in corso di validità di chi fa la richiesta;
- fotocopia di documento di identità in corso di validità dell'Interessato;
- delega scritta dell'Interessato.

Quest'ultimo elemento dovrà essere sostituito dalla prova di un mandato rilasciato in vita o dalla prova del rapporto di parentela, nel caso di diritti riguardanti persone decedute, così come previsto dall'art. 2-*terdecies* del Codice Privacy, introdotto con D.Lgs. 10 agosto 2018 n. 101.
Nei casi in cui la documentazione pervenuta non dovesse risultare adeguata, il Titolare del trattamento richiede all'Interessato l'integrazione della stessa con le informazioni mancanti. In caso di rifiuto da parte del richiedente, il Titolare del trattamento procede a rigettare la richiesta.

5.4 Verifica della validità della richiesta

A seguito della presa in carico della richiesta dell'Interessato, il Titolare del trattamento e/o il *Data Protection Officer* a ciò preposto deve verificare la validità della stessa, accertandosi dell'effettiva esistenza del diritto dell'Interessato. Tale verifica deve essere portata avanti sulla base dei seguenti parametri:

- esistenza dei dati che riguardano l'Interessato;
- contenuto dei dati che riguardano l'Interessato (dati personali comuni, particolari).

Una volta verificata l'esistenza dei presupposti minimi per la gestione della richiesta proveniente dall'Interessato, a seconda della tipologia di richiesta, il Titolare del trattamento o il DPO compilano la tabella "Richieste diritti interessati GDPR".

5.5 Gestione della richiesta

Il Titolare del trattamento o il DPO, sulla base dei trattamenti associati all'Interessato che effettua la richiesta, individua le funzioni aziendali coinvolte nel trattamento dei dati.
Per ogni funzione aziendale identificata il Titolare del trattamento o il DPO invia una richiesta specifica che consiste nella verifica della presenza di dati personali e l'identificazione di tali dati. Qualora la funzione aziendale identificata dovesse riscontrare la presenza di dati all'interno di sistemi e/o archivi di terze parti, dovrà comunicare a suddette terze parti l'esistenza di una richiesta di esercitazione di diritti da parte dell'Interessato, al fine di eseguire una verifica completa della presenza dei dati elettronici relativi all'Interessato, il Titolare del trattamento o il DPO contatta sempre anche la funzione IT che effettua le verifiche all'interno dei *database* aziendali.
Le funzioni aziendali identificate e la funzione IT preposte, al termine della loro ricognizione, comunicano al Titolare del trattamento o al DPO l'esito delle loro analisi, contenente il dettaglio di tutti i dati personali trattati in relazione all'Interessato richiedente.

Nel caso di esercitazione del *Diritto di accesso*, la risposta all'Interessato contiene i dettagli relativi ai dati trattati. La comunicazione dei dati richiesti dall'Interessato deve avvenire mediante formato elettronico: il Titolare del trattamento o il DPO trasferisce i dati all'Interessato presso i recapiti e-mail. Qualora ciò non sia possibile, il Titolare o il DPO trasferisce i dati su apposito supporto removibile e li spedisce, previa verifica dei recapiti con l'Interessato, all'indirizzo di posta indicato.
Il contenuto della comunicazione deve contenere una copia integrale e completa delle sole informazioni richieste (segregare dati di terzi e le valutazioni del Titolare o del DPO) e, allo stesso tempo, non recare danno ai diritti e alle libertà altrui.

Nel caso di esercitazione del *Diritto di rettifica* il Titolare del trattamento o il DPO valuta e autorizza la validità della richiesta di rettifica dei dati. Tale valutazione, a seconda della complessità, viene svolta sulla

base delle normative vigenti, ascoltate le necessità delle funzioni di business. Il Titolare del trattamento o il DPO comunica all'Interessato il rigetto della richiesta di rettifica o l'avvenuta rettifica dei dati trattati.

Nel caso di esercitazione del *Diritto di cancellazione* (*Diritto all'oblio*) il Titolare del trattamento o il DPO deve verificare l'esistenza o meno di una base giuridica tale per cui l'Interessato possa legittimamente opporsi al trattamento. Le casistiche sono definite dall'art. 17 del GDPR.

Qualora la richiesta sia valida (secondo quanto definito al comma 1) e non vi siano ragioni ostative all'accoglimento della richiesta (secondo quanto definito al comma 3), il Titolare del trattamento o il DPO procede nei suoi *database* e chiede lo stesso nei *database* delle terze parti. In caso contrario, rigetta la richiesta e da comunicazione all'Interessato. A conclusione della cancellazione, le funzioni preposte all'evasione della richiesta, invieranno la conferma dell'avvenuta esecuzione dell'operazione al Titolare del trattamento o al DPO che comunicherà l'avvenuta cancellazione all'Interessato.

Nel caso di esercitazione del *Diritto alla limitazione* del trattamento dei dati personali, il Titolare del trattamento o il DPO deve verificare l'esistenza o meno di una base giuridica tale per cui l'Interessato possa legittimamente opporsi al trattamento. Le casistiche sono definite dall'art. 18 del GDPR.
Qualora la richiesta sia valida (secondo quanto definito al comma 1), il Titolare del trattamento o il DPO procede a trattare la richiesta. In caso contrario, rigetta la richiesta e dà comunicazione all'Interessato.
Una volta verificate l'esistenza del diritto e la validità della richiesta dell'Interessato, il Titolare del trattamento o il DPO comunica alle funzioni di *business* coinvolte e alla funzione IT la necessità di limitare il trattamento dei dati personali. Le suddette funzioni definiscono le modalità attraverso le quali limitare il trattamento. A titolo esemplificativo e non esaustivo, il trattamento può essere limitato tramite:

- trasferimento dei dati verso un altro sistema che renda impossibile procedere al trattamento;
- limitazione degli accessi al dato da parte degli utenti e degli autorizzati al trattamento;
- rimozione temporanea dei dati presenti *online* o presso i siti web.

La valutazione della modalità di limitazione deve sempre prevedere il coinvolgimento di tutte le funzioni coinvolte (Titolare, IT, *business*) e il processo decisionale deve essere documentato attraverso opportune evidenze e fogli di lavoro. I dati relativi al trattamento limitato, devono essere opportunamente contrassegnati per renderne agevole il riconoscimento in vista di un possibile rispristino degli stessi.
A conclusione del processo di limitazione del trattamento, il Titolare del trattamento o il DPO comunica l'avvenuta attività all'Interessato.

Nel caso di esercitazione del *Diritto alla portabilità* dei dati personali, il Titolare del trattamento o il DPO deve verificare l'esistenza o meno di una base giuridica tale per cui l'Interessato possa legittimamente richiedere la portabilità dei propri dati al trattamento.
Qualora la richiesta sia valida (secondo quanto definito al comma 1), il Titolare del trattamento o il DPO

procede a trattare la richiesta. In caso contrario, rigetta la richiesta e dà comunicazione all'Interessato.
Il Titolare del trattamento o il DPO trasferisce all'Interessato o, laddove così indicato dallo stesso, al nuovo Titolare del trattamento, i dettagli relativi ai dati trattati. Il trasferimento dei dati richiesti dall'Interessato deve avvenire mediante formato elettronico: il Titolare del trattamento o il DPO trasferisce i dati su apposito supporto removibile e li spedisce, previa verifica dei recapiti con l'Interessato, all'indirizzo di posta indicato.

Il contenuto della comunicazione deve contenere una copia integrale e completa delle sole informazioni richieste e, allo stesso tempo, non recare danno ai diritti e alle libertà altrui.

È necessario verificare che il formato sia interoperabile con i sistemi verso i quali suddetti dati devono essere trasferiti, verificando con il nuovo Titolare indicato dall'Interessato che sia tecnicamente possibile.
A conclusione del processo di trasferimento, il Titolare del trattamento o il DPO comunica l'avvenuta attività all'Interessato.

Nel caso di esercitazione del *Diritto alla opposizione* al trattamento dei dati personali, l'operatore deve verificare l'esistenza o meno di una base giuridica tale per cui l'Interessato possa legittimamente opporsi al trattamento. Le casistiche sono definite dall'art. 21 del GDPR.
Qualora la richiesta sia valida (secondo quanto definito al comma 1), il Titolare del trattamento o il DPO procede a trattare la richiesta. In caso contrario, rigetta la richiesta e dà comunicazione all'Interessato.
A conclusione del processo, il Titolare del trattamento o il DPO, invia la conferma dell'avvenuta esecuzione dell'operazione richiesta all'Interessato.

Tutte le richieste ricevute vengono registrate nella tabella "Richieste diritti interessati GDPR".
Ogni richiesta pervenuta viene numerata e registrata con le seguenti informazioni:

- n. di richiesta;
- data di ricevimento;
- nome della persona o della funzione che ha ricevuto la richiesta;
- data della richiesta;
- nome dell'Interessato;
- nome del delegato se esiste;
- inserire la modalità di comunicazione: telefonica o scritta;
- dati di riconoscimento;
- tipologia del diritto esercitato;
- inserire la presenza del documento di identità;
- inserire la presenza della delega con relativo documento di identità;
- eventuale diniego della risposta;
- contenuto della risposta;
- data della risposta;

- varie.

5.6 Risposta e rispetto delle tempistiche

Le richieste da parte dell'Interessato devono essere evase (anche in caso di diniego) senza ingiustificato ritardo, ovvero entro 30 giorni. Qualora dovessero verificarsi situazioni di particolare complessità, il Titolare del trattamento o il DPO valuta i tempi di risposta e informa l'Interessato.
Una volta correttamente catalogata e indirizzata, la richiesta pervenuta dall'Interessato deve essere intelligibile, concisa, trasparente, facilmente accessibile e utilizzare un linguaggio semplice e chiaro. Viene evasa per iscritto (anche per via informatica) secondo le procedure specificamente definite per ogni tipologia di richiesta.

5.7 Formazione aziendale

Qualora si verifichi uno scenario differente da quello descritto nella precedente procedura, colui/colei che si trovasse a ricevere una richiesta da parte di un Interessato dovrà immediatamente comunicare allo stesso l'esistenza di canali specifici dedicati alla privacy, indicandone gli estremi via e-mail alisei@aliseisgr.it.
Per tale motivo, tutto il personale deve essere formato e informato relativamente all'esistenza di appositi canali di comunicazione per la gestione delle richieste degli Interessati.

ALLEGATO 4

REGISTRO RICHIESTE DIRITTI DEGLI INTERESSATI

Tipologia del diritto	Documento d'identità interessato	Delega e documento d'identità delegato	Eventuale diniego della risposta	Contenuto della risposta	Data della risposta	Varie